arXiv:1006.5959v1 [math.AG] 30 Jun 2010

FINITE GROUP SUBSCHEMES OF ABELIAN VARIETIES OVER FINITE FIELDS

SERGEY RYBAKOV

Abstract. Let A be an abelian variety over a finite field k. The k-isogeny class of A is uniquely determined by the Weil polynomial f_A. We assume that f_A has no multiple roots. For a given prime number $\ell \neq \operatorname{char} k$ we give a classification of groupschemes $B[\ell]$, where B runs through the isogeny class, in terms of certain Newton polygons associated to f_A. As an application we classify zeta functions of Kummer surfaces over k.

1. Introduction.

Let A be an abelian variety over a finite field $k = \mathbb{F}_q$. Let $A[m]$ be the group subscheme of A annulated by m. Fix a prime number $\ell \neq p = \operatorname{char} k$. We say that $A[\ell]$ is the *ℓ-torsion of A*. Suppose that the endomorphism algebra of A over k is commutative. In this paper we classify ℓ-torsion of varieties from the k-isogeny class of A. This result is similar to the classification of groups of k-points $A(k)$ (see [Ry10]). These two problems are closely related, but the former one seems to be easier. For example, we give a full classification of ℓ-torsion for abelian surfaces, but so far we have no idea how to describe groups of k-points on abelian surfaces belonging to a particular nonsimple isogeny class.

The paper is organized as follows. In section 2 we introduce some notation and prove several preliminary results. In particular we reduce the problem to a particular linear algebra question. We give here a simplified version of this question. Let N be a nilpotent $d \times d$ matrix over $\mathbb{F}_\ell$, and let $Q \in \mathbb{Z}_\ell[t]$ be a polynomial of degree d without multiple roots such that $Q \equiv t^d \bmod \ell$. Is it possible to find a matrix M over $\mathbb{Z}_\ell$ such that the characteristic polynomial of M is Q, and $M \equiv N \bmod \ell$? We will refer to this question as *lifting of the nilpotent matrix N to $\mathbb{Z}_\ell$ with respect to Q*.

In section 3 we associate to a nilpotent matrix N a polygon of special type. Let $m_1 \geq \cdots \geq m_r$ be the dimensions of the Jordan cells of N. The numbers $m_1, \ldots, m_r$ determine the matrix up to conjugation. *The Young polygon* $\operatorname{Yp}(N)$ of N is the convex polygon with vertices $(\sum_{j=1}^{i} m_j, i)$ for $0 \leq i \leq r$. For a polynomial $Q \in \mathbb{Z}[t]$ we denote by $\operatorname{Np}_\ell(Q)$ the Newton polygon of Q with respect to ℓ (see Section 3 for a precise definition). The main result of section 3 can be reformulated as follows: one can lift N to $\mathbb{Z}_\ell$ with respect to Q if and only if $\operatorname{Np}(Q)$ lies on or above $\operatorname{Yp}(N)$ (see Theorems 3.2 and 3.3). This result allows one to classify ℓ-torsion of abelain varieties belonging to an isogeny class corresponding to the Weil polynomial without multiple roots.

In section 4 we establish a relationship between Young polygons for the Frobenius actions on an abelian variety and its dual. We also treat the following question due to B. Poonen: is it true that for an abelian surface A the group of k-rational points $A(k)$ is isomorphic to the the group of k-rational points $\widehat{A}(k)$ on its dual? The answer is no, and we give a counterexample.

1991 *Mathematics Subject Classification.* 14K99, 14G05, 14G15.

Key words and phrases. abelian variety, finite field, Newton polygon, Young polygon.

Supported in part by RFBR grants no. 09-01-12170 and 10-01-93110-CNRSLa.

In section 5 we establish a connection between (generalized) matrix factorizations and Tate modules. This technique turns out to be useful when Weil polynomials have multiple roots.

In section 6 we explicitly classify ℓ-torsion of abelian surfaces. In the final section we apply this result to the classification of zeta functions of Kummer surfaces.

The author is grateful to M.A. Tsfasman for his attention to this work and to A. Kuznetsov and A. Zykin for providing useful corrections and comments on the paper.

2. Preliminaries

Throughout this paper k is a finite field $\mathbb{F}_q$ of characteristic p. Let A and B be abelian varieties over k. Then the group $\mathrm{Hom}(A,B)$ of k-homomorphisms from A to B is finitely generated and torsionfree. The algebra $\mathrm{End}^\circ(A) = \mathrm{Hom}(A,A)\otimes_{\mathbb{Z}}\mathbb{Q}$ contains the Frobenius endomorphism F, its center is equal to $\mathbb{Q}[F]$, and the center of $\mathrm{End}^\circ(A)\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$ is $\mathbb{Q}_\ell[F]$.

Let A be an abelian variety of dimension g over a field k, and let $\bar{k}$ be an algebraic closure of k. For a natural number m denote by A_m the kernel of multiplication by m in $A(\bar{k})$. Let $A[m]$ be the group subscheme of A, which is the kernel of multiplication by m. By definition $A_m = A[m](\bar{k})$. For any prime $\ell \neq p$ let $T_\ell(A) = \varprojlim A_{\ell^r}$ be the Tate module of A, and let $V_\ell(A) = T_\ell(A)\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell$ be the corresponding vector space over $\mathbb{Q}_\ell$. Then $T_\ell(A)$ is a free $\mathbb{Z}_\ell$-module of rank $2g$. The Frobenius endomorphism F of A acts on the Tate module by a semisimple linear operator, which we also denote by $F : T_\ell(A) \to T_\ell(A)$. The characteristic polynomial

$$f_A(t) = \det(t - F)$$

is called *the Weil polynomial of* A. It is a monic polynomial of degree $2g$ with rational integer coefficients independent of the choice of prime ℓ. It is well known that for isogenous varieties A and B we have $f_A(t) = f_B(t)$. Tate proved that the isogeny class of an abelian variety is determined by its characteristic polynomial, that is $f_A(t) = f_B(t)$ implies that A is isogenous to B. The polynomial f_A has no multiple roots if and only if the endomorphism algebra $\mathrm{End}^\circ(A)$ is commutative (see [WM69]).

Thus we have a nice description of isogeny classes of abelian varieties over k in terms of Weil polynomials. It looks natural to consider classification problems concerning abelian varieties inside a given isogeny class. Our goal is to describe ℓ-torsion of abelian varieties. First we reduce the problem to a linear algebra problem in a sequence of steps.

Reduction step 0. A finite etale groupscheme G over k is uniquely determined by the Frobenius action on $G(\bar{k})$ (see [De78]). If $\ell \cdot G = 0$, then $G(\bar{k})$ is an $\mathbb{F}_\ell$-vector space and Frobenius action is $\mathbb{F}_\ell$-linear. By definition of the Tate module, we have $A[\ell](\bar{k}) \cong T_\ell(A)/\ell T_\ell(A)$. Thus the structure of a group scheme on $A[\ell]$ depends only on the module structure on $T_\ell(A)$ over $R = \mathbb{Z}_\ell[F]$. Moreover, since the action of F on $V_\ell(A)$ is semisimple, we know the structure of the R-module on $V_\ell(A)$. Let

$$f_A = \prod_{j=1}^{s} f^{(j)},$$

where $f^{(j)}$ divides $f^{(j-1)}$, and suppose that $f^{(j)}$ has no multiple roots for $1 \leq j \leq s$. Then

$$V_\ell(A) \cong \oplus_j \mathbb{Q}_\ell[t]/f^{(j)}(t)\mathbb{Q}_\ell[t]$$

as R-modules, where F acts on the right by multiplication by t.

The following lemma shows what R-modules can arise as Tate modules of varieties from a fixed isogeny class.

Lemma 2.1. [Mil08, IV.2.3] *If $f : B \to A$ is an isogeny then, $T_\ell(f) : T_\ell(B) \to T_\ell(A)$ is an embedding of R-modules, and if T denotes its image then*

$$F(T) \subset T \quad \text{and} \quad T \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell. \tag{1}$$

Conversely, if $T \subset T_\ell(A)$ is a $\mathbb{Z}_\ell$-submodule such that (1) holds, then there exists an abelian variety B defined over k and an isogeny $f : B \to A$ such that $T_\ell(f)$ induces an isomorphism $T_\ell(B) \cong T$. □

Lemma 2.2. *Let S be a complete local ring with maximal ideal $\mathfrak{p}$. Suppose we are given a family of polynomials $P_i, h_i \in S[t]$ such that $P_i \equiv h_i^{d_i} \mod \mathfrak{p}$, and h_i are pairwise coprime modulo $\mathfrak{p}$. Then*

$$S[t]/\prod P_i S[t] \cong \prod S[t]/P_i(t)S[t].$$

Proof. Note that P_i generate pairwise comaximal ideals in $S[t]$, i.e. $P_iS[t] + P_jS[t] = S[t]$ for $i \neq j$. Indeed, $g_1P_i + g_2P_j \equiv 1 \mod \mathfrak{p}$ for some polynomials g_1 and $g_2 \in \mathbb{Z}_\ell[t]$. Clearly, this is an upper triangular system of linear congruences on the coefficients of g_1. By Hensel lemma one can change coefficients of g_1 to get an equality $g_1P_i + g_2P_j = 1$. The lemma follows by the Chinese remainder theorem. □

Reduction step 1. Let T be a Tate module. Suppose we are given a family of polynomials $P_i, h_i \in S[t]$ as in Lemma 2.2 such that $f^{(1)}(t) = \prod P_i$. Take

$$R_i = \mathbb{Z}_\ell[t]/P_i(t)\mathbb{Z}_\ell[t].$$

It follows that $T = \oplus T_i$, where $T_i = R_iT$ is an R_i-module for any i. Moreover, the image of t in R_i acts on T_i as Frobenius. We have reduced our task to the following question. Let $f \in \mathbb{Z}_\ell[t]$ satisfy $f(t) \equiv h(t)^d \mod \ell$, where $h(t) \in \mathbb{Z}_\ell[t]$ is irreducible modulo ℓ. Suppose

$$f = \prod_{j=1}^{s} f^{(j)},$$

where $f^{(j)}$ divides $f^{(j-1)}$, and suppose that $f^{(j)}$ has no multiple roots for $1 \leq j \leq s$. Take

$$R = \mathbb{Z}_\ell[t]/f^{(1)}(t)\mathbb{Z}_\ell[t].$$

Classify all possible modules of the form $T/\ell T$, where T is an R-invariant $\mathbb{Z}_\ell$-lattice in

$$V = \oplus_j \mathbb{Q}_\ell[t]/f^{(j)}(t)\mathbb{Q}_\ell[t].$$

The polynomial h is irreducible modulo ℓ, thus by [KF67, Proposition I.7.1] the field

$$L = \mathbb{Q}_\ell[t]/h(t)\mathbb{Q}_\ell[t]$$

is an unramified extension of $\mathbb{Q}_\ell$. Denote by S the ring of integers of L. Then $T \otimes_{\mathbb{Z}_\ell} S$ is an $R \otimes_{\mathbb{Z}_\ell} S$-invariant $\mathbb{Z}_\ell$-lattice in $V \otimes_{\mathbb{Z}_\ell} S$. If $h(t) \equiv \prod_i (t - \alpha_i) \mod \ell$, then $f^{(j)}(t) \equiv \prod f_i^{(j)}(t)$ such that $f_i^{(j)} \in S[t]$ and

$$f_i(t) = \prod_j f_i^{(j)}(t) \equiv (t - \alpha_i)^d \mod \ell.$$

By Lemma 2.2

$$R \otimes_{\mathbb{Z}_\ell} S \cong \prod S[t]/f_i(t)S[t],$$

and as before $T \otimes_{\mathbb{Z}_\ell} S \cong \oplus T_i$, where T_i is an $S[t]/f_i(t)S[t]$-module. Note that $T_i \cong T$ as R-modules, and

$$R \cong S[t]/f_1^{(1)}S[t].$$

The polynomial $Q(t) = f_1(t + \alpha_1)$ is the characteristic polynomial of the action of $F - \alpha_1$ on T_1.

Definition 2.3. We call the triple (f, h, Q) *a distinguished triple of polynomials*, if

(1) polynomials $f, h \in \mathbb{Z}_\ell[t]$ are monic, and $S = \mathbb{Z}_\ell[t]/h(t)\mathbb{Z}_\ell[t]$ is a regular local ring with unramified fraction field;
(2) $f(t) \equiv h(t)^d \mod \ell$;
(3) $Q \in S[t]$, and $Q(t) \equiv t^d \bmod \ell$.
(4) Suppose $f = \prod f_i$ as before, and $h(t) \equiv \prod_i (t - \alpha_i) \mod \ell$; then $Q(t) = f_1(t + \alpha_1)$.

Reduction step 2. Let T be a direct (F-equivariant) summand of a Tate module as in step 1. If f has no multiple roots, then $T \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong R \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, and our problem reduced to the following linear algebra problem. Let (f, h, Q) be a distinguished triple of polynomials, and let $V = R \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ be a $\mathbb{Q}_\ell$-vector space with an action of R. Describe all finite R-modules (up to isomorphism) of the form $T/\ell T$, where T is an arbitrary R-invariant S-lattice in V.

If we choose a basis of T, the problem can be reformulated as follows. Let N be a matrix of the action of $F - \alpha_1$ on $T/\ell T$ in some basis over the finite field $S/\ell S$. It is a nilpotent matrix over $S/\ell S$, since $Q \equiv t^d \bmod \ell$. Is it possible to find a matrix M over S such that $Q(t) = \det(t - M)$, and $M \equiv N \bmod \ell$? We will refer to this question as *lifting of nilpotent matrix N to S with respect to Q*.

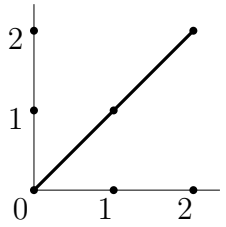
3. Finite group subschemes of abelian varieties

Let L be an unramified extension of $\mathbb{Q}_\ell$, and let S be its ring of integers. Let $Q \in S[t]$ be a polynomial of degree d such that $Q \equiv t^d \mod \ell$, and let N be a nilpotent $d \times d$ matrix over $S/\ell S$. In this section we give a partial answer to the question: when is it possible to lift N to S with respect to Q? Using this result we get a classification of group schemes of the form $A[\ell]$ for A from a fixed isogeny class such that f_A has no multiple roots.

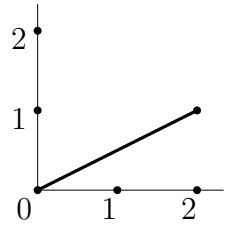
First we associate to N a polygon of special type.

Definition 3.1. Let N be a nilpotent $d \times d$ matrix over a field, and let $m_1 \geq \cdots \geq m_r$ be the dimensions of its Jordan cells. The numbers $m_1, \ldots, m_r$ determine this matrix up to conjugation. *The Young polygon* $\mathrm{Yp}(N)$ of N is the convex polygon with vertices $(\sum_{j=1}^{i} m_j, i)$ for $0 \leq i \leq r$. We write $\mathrm{Yp}(N) = (m_1, \ldots, m_r)$.

The Young polygon has $(0, 0)$ and (d, r) as its endpoints, and its slopes are $1/m_1, \ldots, 1/m_r$. For example, the following picture shows Young polygons for the zero and a nonzero 2×2 nilpotent matrixes.



Pic. 1



Pic. 2

We will use the following notation. Let T be a finitely generated free S-module, and let E be an S-linear endomorphism of T that induces on $T/\ell T$ a nilpotent endomorphism with matrix N in some basis. By definition, $\mathrm{Yp}(E|T) = \mathrm{Yp}(N)$. Clearly, this definition does not depend on a choice of basis.

Denote by ν the normalized valuation on L, i.e. $\nu(\ell) = 1$. Let $Q(t) = \sum_i Q_i t^{d-i}$ be a polynomial of degree d over L. Take the lower convex hull of the points $(i, \nu(Q_i))$ for $0 \leq i \leq$

$\deg Q$ in $\mathbb{R}^2$. The boundary of this region is called *the Newton polygon* $\mathrm{Np}(Q)$ *of* Q. Its vertices have integer coefficients, and $(0,0)$ and $(d,\nu(Q_d))$ are its endpoints. The *slopes of* Q are the slopes of this polygon. Note that each slope λ_i has a multiplicity. We always assume that $\lambda_1 \le \cdots \le \lambda_r$, and write

$$\mathrm{Np}(Q) = (\lambda_1, \dots, \lambda_r).$$

Theorem 3.2. *Let T be a finitely generated free S-module, and let x be a linear operator on T. Suppose $Q(t) = \det(t - x|T \otimes_S L)$ is the characteristic polynomial of the action of x on T. Then* $\mathrm{Np}(Q)$ *lies on or above* $\mathrm{Yp}(x|T)$.

Proof. Let $\mathrm{Yp}(x|T) = (m_1, \dots, m_r)$. By Nakayama lemma there exist generators $v_1, \dots, v_r$ of T over R such that

$$v_1, xv_1 \dots, x^{m_1-1}v_1, \dots, v_r, \dots, x^{m_r-1}v_r$$

give a Jordan basis in $T/\ell T$ for x. Let H be a matrix of x in this basis and let $H_{i_1,\dots,i_m}$ be the determinant of the submatrix of H cut by the columns and rows with the numbers $i_1, \dots, i_m$. The characteristic polynomial of x acting on T is

$$Q(t) = \sum_{i=0}^{d} a_i t^{d-i},$$

and

$$a_m = (-1)^m \sum_{i_1 < \cdots < i_m} H_{i_1,\dots,i_m}.$$

It follows that

$$\nu(a_m) \ge \min_{i_1 < \cdots < i_m} \nu(H_{i_1,\dots,i_m}).$$

Let $m = m_1 + \cdots + m_{s-1} + a$, where $0 < a \le m_s$. We have to show that if $H_{i_1,\dots,i_m} \ne 0$, then $\nu(H_{i_1,\dots,i_m}) \ge s$. Note that if $i \ne m_1 + \cdots + m_j$ for all j, then the i-th column of H has 1 only in the position number $i+1$, and its other entries are zero. Thus if $i \in \{i_1, \dots, i_m\}$, and $H_{i_1,\dots,i_m} \ne 0$, then $i+1 \in \{i_1, \dots, i_m\}$. If $i = m_1 + \cdots + m_j$ for some j, then ℓ divides the i-th column. We see that if $H_{i_1,\dots,i_m} \ne 0$, then the set $\{i_1, \dots, i_m\}$ is a union of *blocks*. Each block is an interval

$$\{i, i+1, \dots, m_1 + \cdots + m_j\}$$

of length not greater than m_j. If $m > m_1 + \cdots + m_{s-1}$, then the set $\{i_1, \dots, i_m\}$ contains no less then s blocks, and $\nu(H_{i_1,\dots,i_m}) \ge s$. Thus if $(m, \nu(a_m))$ is a vertex of $\mathrm{Np}(Q)$ then $\nu(a_m) \ge s$, and $\mathrm{Np}(Q)$ lies on or above $\mathrm{Yp}(x|T)$. □

Theorem 3.3. *Let $R = S[t]/Q(t)S[t]$, and let $V = R \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Let N be a nilpotent matrix such that* $\mathrm{Np}(Q)$ *lies on or above* $\mathrm{Yp}(N)$. *Then there exists an R-lattice T in V such that* $\mathrm{Yp}(x|T) = \mathrm{Yp}(N)$.

Proof. Recall that $Q = \det(t - x|V)$ is the minimal polynomial of the action of x on V. Let $\mathrm{Yp}(N) = (m_1, \dots, m_r)$. First we construct the generators $v_1, \dots, v_r$ of T in V such that $R \subset T \subset V$. Let $m = m_1 + \cdots + m_s$, and let $Q(t) = \sum_{i=0}^{d} a_i t^{d-i}$. For $1 \le s \le r$ we put

$$v_{s+1} = \frac{x^m + \sum_{j=1}^{m} a_j x^{m-j}}{\ell^s}.$$

Finally, let $v_1 = 1$, and let $v_{r+1} = 0$. Note that

$$v_1, xv_1 \dots, x^{m_1-1}v_1, \dots, v_r, \dots, x^{m_r-1}v_r$$

have different degrees viewed as polynomials in x, and hence generate T over S.

Now we prove that T is an R-module. The point $(m-m_s, s-1)$ is a vertex of $\mathrm{Yp}(N)$. By assumption $\mathrm{Np}(Q)$ lies on or above $\mathrm{Yp}(N)$, thus $(m-m_s, s-1)$ is not higher than $\mathrm{Np}(Q)$. It follows that ℓ^s divides a_j for all $j > m-m_s$. Thus

$$u_s = \frac{\sum_{j=m-m_s+1}^{m} a_j x^{m-j}}{\ell^s} \in S \cdot 1 \subset T.$$

Moreover,

$$x^{m_s} v_s = \ell(v_{s+1} - u_s) \in \ell T.$$

This proves that $xT \subset T$, and that $\mathrm{Yp}(x|T) = \mathrm{Yp}(N)$. □

It follows that one can lift N to S with respect to Q if and only if $\mathrm{Np}(Q)$ lies on or above $\mathrm{Yp}(N)$.

Example 3.4. Let $Q(t) = t^2 - \ell t - \ell$. Its Newton polygon is drawn on Picture 2. Then we can lift the nonzero nilpotent Jordan cell (its Young polygon is equal to $\mathrm{Np}(Q(t))$). For example, take

$$M = \begin{pmatrix} 0 & \ell \\ 1 & \ell \end{pmatrix}.$$

Clearly, $Q(t) = \det(t - M)$. We can not lift the zero matrix, because its Young polygon (see Pic. 1) is higher than $\mathrm{Np}(Q)$.

Let E be an endomorphism of a vector space V with characteristic polynomial $h(t) = t^d + a_{d-1}t^{d-1} + \dots a_1 t + a_0$. It is well known that if h has no multiple roots, then in some basis the matrix of E is the companion matrix $M(h)$ of h (see [HK71]):

$$\begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -a_{d-2} \\ & & & 1 & -a_{d-1} \end{pmatrix}$$

Let I_m be the identity matrix of dimension m. For a polynomial $h \in \mathbb{Z}_\ell[t]$ we denote its reduction modulo ℓ by $\bar{h} \in \mathbb{F}_\ell[t]$.

Let (f, h, Q) be a distinguished triple of polynomials. We use the notation of section 2. The following simple proposition allows one to compute a matrix of the Frobenius endomorphism.

Proposition 3.5. *Let N be the matrix of x in some basis of $T/\ell T$ over S. Then in some basis of $T/\ell T$ over $\mathbb{F}_\ell$ the element $F = x + \alpha$ acts with matrix $M(\bar{h}) \otimes I_d + I_{\deg h} \otimes N$.* □

Proof. We know that α acts on $S/\ell S$ with matrix $M(\bar{h})$ in some basis over $\mathbb{F}_\ell$. Thus α acts on $T/\ell T$ with matrix $M(\bar{h}) \otimes I_d$. On the other hand, x acts on $T/\ell T$ with matrix $I_{\deg h} \otimes N$ in some basis over $\mathbb{F}_\ell$. □

Recall that the groupschemes we are interested in are uniquely determined by the linear Frobenius action on the group of $\bar{k}$-points. Let N be a nilpotent $d \times d$-matrix.

Definition 3.6. *A distinguished groupscheme* (associated to (f, h, Q) and N) is a finite etale groupscheme $A(f, N)$ over k such that $\dim_{\mathbb{F}_\ell} A(f, N)(\bar{k}) = \deg f$, and F acts on $A(f, N)(\bar{k})$ with the matrix $M(\bar{h}) \otimes I_d + I_{\deg h} \otimes N$ in some basis, where $\mathrm{Np}(Q)$ lies on or above $\mathrm{Yp}(N)$.

Note that for a given f the polynomial h in a distinguished triple (f, h, Q) is uniquely determined modulo ℓ. Thus $A(f, N)$ is uniquely determined by f and N up to an isomorphism.

Combining Theorems 3.2 and 3.3 with results of section 2 we obtain the following corollaries.

Corollary 3.7. *Let A be an abelian variety over k. Let (f_i, h_i, Q_i) be a family of distinguished triples of polynomials such that the Weil polynomial $f_A = \prod_i f_i$, and h_i are pairwise coprime modulo ℓ. Then $A[\ell] \cong \oplus A(f_i, N_i)$ is a sum of distinguished groupschemes.*

Proof. Let $S_i = \mathbb{Z}_\ell[t]/h_i(t)\mathbb{Z}_\ell[t]$, and let $R_i = S[t]/Q_i(t)S[t]$. By Lemma 2.2 $T_\ell(A) \cong \oplus T_i$, where $T_i = R_i T$ is an R_i-module. For any i let π_i be the image of t in R_i, and let $f_i \equiv h_i^{d_i} \mod \ell$. Then by Proposition 3.5 and Theorem 3.2 π_i acts on $T_i/\ell T_i$ with the matrix $M(\bar{h}_i) \otimes I_{d_i} + I_{\deg h_i} \otimes N_i$, where N_i is a nilpotent matrix such that $\mathrm{Np}(Q_i)$ lies on or above $\mathrm{Yp}(N_i)$. □

Corollary 3.8. *Let A be an abelian variety over k. Suppose f_A has no multiple roots. Let (f_i, h_i, Q_i) be a family of distinguished triples of polynomials such that $f_A = \prod_i f_i$, and h_i are pairwise coprime modulo ℓ. Then for any family of distinguished groupschemes $A(f_i, N_i)$ there exists an abelian variety B isogenous to A such that $B[\ell] \cong \oplus A(f_i, N_i)$.*

Proof. Since f_A has no multiple roots, $V_\ell(A) \cong \mathbb{Q}_\ell[t]/f_A(t)\mathbb{Q}_\ell[t]$. As before, let $S_i = \mathbb{Z}_\ell[t]/h_i(t)\mathbb{Z}_\ell[t]$, and let $R_i = S[t]/Q_i(t)S[t]$. Then $V_\ell(A) \cong \oplus V_i$, where $V_i = R_i V$ is an R_i-module. Let α_i be a root of h_i. By Theorem 3.3 there exists an S_i-lattice $T_i \subset V_i$ such that $F - \alpha_i$ acts on $T_i/\ell T_i$ with matrix N_i in some basis over $S_i/\ell S_i$. Let $T = \oplus T_i$, then by Proposition 3.5 F acts on $T/\ell T$ with matrix $\oplus_i (M(\bar{h}_i) \otimes I_{\deg Q_i} + I_{\deg h_i} \otimes N_i)$. By Lemma 2.1 there exists a variety B such that $T \cong T_\ell(B)$. □

For the proof of the previous corollary we need the lift M of a nilpotent matrix with respect to Q to be semisimple, because the Frobenius action is semisimple on $V_\ell(A)$. On the other hand, if Q has multiple roots then the construction of Theorem 3.3 never gives a semisimple matrix. If $Q = P^s$, and $P \in S[t]$ has no multiple roots, we may apply the following construction to obtain a semisimple lift M. Let N_j be a family of nilpotent matrices for $1 \le j \le s$ such that $\mathrm{Np}(P))$ lies on or above $\mathrm{Yp}(N_j)$. Then the argument of Theorem 3.3 gives latices T_j such that $\mathrm{Yp}(x| \oplus T_j) = \mathrm{Yp}(\oplus N_j)$. For a general P we do not obtain all possible actions of x on $T/\ell T$, but obviously we have the following result.

Proposition 3.9. *Let $\deg P = 2$. There exists an S-lattice T of rank $2r$ such that x acts on $T/\ell T$ with a matrix N in some basis if and only if $\mathrm{Np}(P^r)$ lies on or above $\mathrm{Yp}(N)$, and all slopes of $\mathrm{Yp}(N)$ are equal to $1/2$ or 1.* □

Proof. Suppose such a lattice T exists. Since $\deg P = 2$, any Jordan cell of N has dimension at most 2. Conversely, $N = \oplus N_i$, where each N_i is a 2×2 nilpotent matrix. By Theorem 3.3 for any i there exists an S-lattice T_i such that x acts on $T_i/\ell T_i$ with the matrix N_i. Then $T = \oplus T_i$. □

4. Young polygons and duality.

By $\widehat{A}$ we denote the dual variety of an abelian variety A. Suppose (f, h, Q) is a distinguished triple of polynomials such that f divides f_A, and polynomials f and f_A/f have no common roots modulo ℓ. By lemma 2.2 there exists a direct summand T of $T_\ell(A)$ such that F acts on T with characteristic polynomial f. Put $\hat{f}(t) = t^{\deg f} f(\frac{1}{t})$, and denote the corresponding direct summand of $T_\ell(\widehat{A})$ for $\widehat{f}$ by $\widehat{T}$.

Proposition 4.1. *Let α be a root of h. Then $\mathrm{Yp}(F - \alpha|T) = \mathrm{Yp}(F - q/\alpha|\widehat{T})$.*

Proof. There is a Weil pairing $e : T_\ell(A) \times T_\ell(\widehat{A}) \to \mathbb{Z}_\ell$ such that $e(Fx, Fy) = qe(x, y)$, where $x \in T_\ell(A)$ and $y \in T_\ell(\widehat{A})$ [Mum70]. Its restriction to $T \times \widehat{T}$ is nondegenerate. Let $S = \mathbb{Z}_\ell[\alpha]$. By an integral version of Deligne trick [BGK06, Lemma 3.1] there exists an S-linear pairing

$e_S : T \times \widehat{T} \to S$ such that $e_S(Fx, Fy) = qe_S(x, y)$ and $e = Tr_{L/\mathbb{Q}_\ell} \circ e_S$, where L is the fraction field of S. We have

$$e_S(Fx, y) = e_S(Fx, F(F^{-1}y)) = e_S(x, (qF^{-1})y).$$

Let $M = \oplus_i (M(\bar{h}_i) \otimes I_{d_i} + I_{\deg h_i} \otimes N_i)$ be the matrix of the action of F on $T/\ell T$ in some basis over $S/\ell S$, and let $\widehat{M}$ be the matrix of the action of F on $\widehat{T}/\ell\widehat{T}$ in the dual basis. It follows that $\widehat{M^t} = qM^{-1}$, where $\cdot^t$ means transpose. We see that for any cell of M corresponding to the nilpotent matrix N_i there exists a cell of $\widehat{M}$ corresponding to the same matrix N_i. The proposition follows. □

We now give an example of an abelian surface A such that the group of points $A(k)$ is not isomorphic to the group of points on the dual surface $\widehat{A}(k)$. Recall that $A(k)$ is a kernel of $1 - F : A \to A$, and the ℓ-component $A(k)_\ell = \ker 1 - F : T_\ell(A) \to T_\ell(A)$.

Example 4.2. Let $q = 7$, and let $\ell = 5$. Suppose $f_a(t) = t^2 + 2t + 7$ and $f_b(t) = t^2 - 3t + 7$ are Weil polynomials of two elliptic curves. The polynomial $f = f_a f_b$ is the Weil polynomial of an abelian surface. Note that $f_a(t) \equiv f_b(t) \equiv (t-1)(t-q) \mod 5$. Thus we have a decomposition $f = f_1 f_2$ over $\mathbb{Z}_5$, where $f_1 \equiv (t-1)^2 \mod 5$, and $f_2 \equiv (t-q)^2 \mod 5$. For any abelian surface B with Weil polynomial f we have a decomposition $T_5(B) \cong T_1 \oplus T_2$, where F acts on T_i with characteristic polynomial f_i for $i = 1, 2$. By Theorem 3.2 $F - 1$ acts on $T_1/5T_1$ trivially and by Theorem 3.3 there exists a lattice T in $T_2 \otimes \mathbb{Q}$ such that $F - q$ acts on $T/5T$ nontrivially. In the first case the Young polygon of $F - 1$ is $(1/2)$, and in the second case the Young polygon of $F - q$ is $(1, 1)$. By Lemma 2.1 there exists an abelian surface A such that $T_5(A) \cong T_1 \oplus T_2$. By the previous proposition $A(\mathbb{F}_7)_5 \cong \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$, and $\widehat{A}(\mathbb{F}_7)_5 \cong \mathbb{Z}/25\mathbb{Z}$.

5. Matrix factorizations.

Let S be the ring of integers in a finite unramified extension L of $\mathbb{Q}_\ell$. Fix a pair of polynomials $f, f_1 \in S[t]$ and a positive integer r. Let $R = S[t]/f_1 S[t]$, and let $\bar{S} = S/\ell S$. Denote by $x \in R$ the image of t under the natural projection from $S[t]$.

Definition 5.1. A matrix factorization (X, Y) is a pair of $r \times r$ matrices with coefficients in S such that $YX = f_1 \cdot I_r$ and $\det X = f$.

A matrix factorization corresponds to a finitely generated R-module T given by the presentation:

$$S[t]^r \xrightarrow{X} S[t]^r \to T \to 0, \tag{2}$$

because we may consider T as an $S[t]$-module which is annihilated by f_1.

Proposition 5.2. *Suppose $f_1 \equiv t^{d_1} \mod \ell$, and $\deg f_1 = d_1$. The module T is free of finite rank d over S, and characteristic polynomial of the action of x on T is equal to f.*

Proof. Since $f_1 \equiv t^{d_1} \mod \ell$ and $\deg f_1 = d_1$, the ring R is generated as S-module by the elements $1, x, \ldots, x^{d_1 - 1}$. By definition, T is a finitely generated R-module, thus it is finitely generated over S.

Take the tensor product of the presentation (2) with $\bar{S}[t]$:

$$\bar{S}[t]^r \xrightarrow{\bar{X}} \bar{S}[t]^r \to T \otimes_S \bar{S} \to 0.$$

The ring $\bar{S}[t]$ is a principal ideal domain, thus there exist matrices M_1 and M_2 over $\bar{S}[t]$ such that $\det M_1 = \det M_2 = 1$ and $M_1 \bar{X} M_2$ is a diagonal matrix with determinant t^d. It follows that $M_1 \bar{X} M_2$ is a diagonal matrix $\operatorname{diag}(x^{m_1}, \ldots, x^{m_r})$ for some $m_1 \ldots, m_r \in \mathbb{N}$. We get

$$T \otimes_S \bar{S} \cong \oplus_{i=1}^r \bar{S}[t]/x^{m_i}\bar{S}[t].$$

By Nakayama lemma T is generated by d elements over S.

Now take a presentation of $T \otimes_S L$:

$$L[t]^r \xrightarrow{X} L[t]^r \to T \otimes_S L \to 0.$$

As before, there exist matrices M_3 and M_4 over $L[t]$ such that $\det M_3 = \det M_4 = 1$ and $M_3 X M_4 = \operatorname{diag}(g_1, \dots, g_r)$. Clearly,

$$T \otimes_S L \cong \oplus_{i=1}^r L[t]/g_i L[t],$$

and $\operatorname{rk} T = d$. This proves that T is free over S. To conclude the prof we recall that the characteristic polynomial of the action of t on $L[t]/g_i L[t]$ is equal to g_i. □

The following proposition shows that modules over R give rise to matrix factorizations.

Proposition 5.3. *Let T be an R-module which is free of finite rank over S. Suppose that T can be generated over R by r elements, and that $\operatorname{Yp}(x|T) = (m_1, \dots, m_r)$. Then there exists a matrix factorization (X, Y) such that T has presentation (2), and*

$$X \equiv \operatorname{diag}(t^{m_1}, \dots, t^{m_r}) \mod \ell.$$

Proof. Let $v_1, \dots, v_r$ be generators of T over R. Then $x^{m_i} v_i = \sum_j a_{ji}(x) v_j$, where $a_{ji} \in S[t]$ and $\deg a_{ji} < m_j$. Take X to be the matrix with entries $t^{m_i}\delta_{ji} - a_{ji}$. Define an R-module T' by the presentation:

$$S[t]^r \xrightarrow{X} S[t]^r \to T' \to 0.$$

Let $m = \sum_i m_i$. Then $\det X \equiv t^m \mod \ell$, and from the inequalities $\deg a_{ji} < m_j$ it follows that $\det X$ is a polynomial of degree m. By Proposition 5.2 T' is a free S module of rank m. By definition of T' we have a surjective map of S-modules $T' \to T$. Since they have the same rank as S-modules this map is an isomorphism, and by Proposition 5.2 $\det X = f$.

Multiplying presentation (2) with f_1 we get a commutative diagram

$$\begin{array}{ccccccc} S[t]^r & \xrightarrow{X} & S[t]^r & \longrightarrow & T & \longrightarrow & 0 \\ {\scriptstyle f_1}\downarrow & & \downarrow{\scriptstyle f_1} & & {\scriptstyle 0}\downarrow & & \\ S[t]^r & \xrightarrow{X} & S[t]^r & \longrightarrow & T & \longrightarrow & 0 \end{array}$$

Since $S[t]^r$ is free, there exists a matrix Y such that the diagram

$$\begin{array}{ccccccc} S[t]^r & \xrightarrow{X} & S[t]^r & \longrightarrow & T & \longrightarrow & 0 \\ & {\scriptstyle Y}\swarrow & \downarrow{\scriptstyle f_1} & & {\scriptstyle 0}\downarrow & & \\ S[t]^r & \xrightarrow{X} & S[t]^r & \longrightarrow & T & \longrightarrow & 0 \end{array}$$

commutes. It follows that $YX = f_1 I_r$. Thus, the pair (X, Y) is a matrix factorization. □

Example 5.4. Let $\deg f_1 = 3$ and $f = f_1^2$. Suppose f_1 has no multiple roots. When there exists an R-module T such that x acts with $r = 3$ Jordan cells of dimension 2? By Proposition 5.3 such a module exists iff there exists a matrix factorization (X, Y) such that

$$X \equiv \operatorname{diag}(t^2, t^2, t^2) \mod \ell.$$

The matrix factorization (Y, X) gives a module T' over R which is generated by 3 elements and the characteristic polynomial of x is equal to $\det Y = f_1^3/f = f_1$. Moreover, $Y \equiv \operatorname{diag}(t, t, t)$ mod ℓ. It follows that $\operatorname{Yp}(x|T') = (1, 1, 1)$. By Theorems 3.2 and 3.3 such a module T' exists iff $\operatorname{Np}(f_1)$ lies on or above $\operatorname{Yp}(x|T')$.

6. ℓ-torsion of abelian surfaces.

In this section we classify ℓ-torsion of abelian surfaces.

Theorem 6.1. *Let A be an abelian surface over k with the Weil polynomial $f_A(t) = t^4 + a_1t^3 + a_2t^2 + qa_1t + q^2$. Suppose first that f_A has no multiple roots, then we have the following five cases:*

- **(1):** *if $f_A(t)$ has no multiple roots modulo ℓ then $A[\ell] \cong A(f_A, 0)$;*
- **(2):** *if $f_A(t) \equiv f_1f_2 \bmod \ell$, where $f_1 \equiv (t-\alpha)^2 \bmod \ell$, and f_2 is irreducible modulo ℓ, then $A[\ell] \cong A(f_2, 0) \oplus A(f_1(t+\alpha), N)$, where N is a nilpotent 2×2 matrix;*
- **(3):** *if $f_A(t) \equiv f_1f_2 \bmod \ell$, where $f_i \equiv (t-\alpha_i)^2 \bmod \ell$, for $i = 1, 2$ and $\alpha_1 \not\equiv \alpha_2 \bmod \ell$, then $A[\ell] \cong A(f_1(t+\alpha_1), N_1) \oplus A(f_2(t+\alpha_2), N_2)$, where N_1 and N_2 are nilpotent 2×2-matrices;*
- **(4):** *if $f_A(t) \equiv h(t)^2 \bmod \ell$, where h is irreducible modulo ℓ, then $A[\ell] \cong A(f_A, N)$, where N is a nilpotent 2×2-matrix. If $\ell \neq 2$, and ℓ^2 does not divide $a_1^2 - 4a_2 + 8q$, or $\ell = 2$, and 4 does not divide $a_1 + a_2 + 1 - 2q$, then $N \neq 0$;*
- **(5):** *if $f_A(t) \equiv (t-\alpha)^4 \bmod \ell$, then $A[\ell] \cong A(f(t+\alpha), N)$, where N is a nilpotent 4×4-matrix.*

Suppose that f_A has multiple roots, then we have the following three cases:

- **(6):** *$f_A = P^2$, where P has no multiple roots. Then*
  - **(a):** *if P has no multiple roots modulo ℓ, then $A[\ell] \cong A(P, 0) \oplus A(P, 0)$;*
  - **(b):** *if $P(t) \equiv (t-\alpha)^2 \bmod \ell$, then $A[\ell] \cong A(P(t+\alpha), N_1) \oplus A(P(t+\alpha), N_2)$, where N_1 and N_2 are nilpotent 2×2-matrixes.*
- **(7):** *$f_A(t) = (t \pm \sqrt{q})^2(t^2 - bt + q)$, where $P_1(t) = t^2 - bt + q$ has no multiple roots. Let $P_2(t) = (t \pm \sqrt{q})^2$.*
  - **(a):** *If $P_1 \not\equiv P_2 \bmod \ell$, and P_1 has no multiple roots modulo ℓ, then $A[\ell] \cong A(P_1, 0) \oplus A(P_2, 0)$.*
  - **(b):** *If $P_1 \not\equiv P_2 \bmod \ell$, and $P_1(t) \equiv (t-\alpha)^2 \bmod \ell$, then $A[\ell] \cong A(P_1(t+\alpha), N) \oplus A(P_2, 0)$, where N is a nilpotent 2×2-matrix.*
  - **(c):** *If $P_1 \equiv P_2 \bmod \ell$, then*
    - **(i):** *either $A[\ell] \cong A(P_1(t+\alpha)t, N) \oplus A(t, 0)$, where N is a 3×3 nilpotent matrix; or*
    - **(ii):** *if ℓ^2 divides $P_1(\mp\sqrt{q})$, then $A[\ell] \cong A(P_1(t+\alpha), N) \oplus A(t^2, N)$, where N is a nonzero 2×2 nilpotent matrix.*
- **(8):** *If $f_A(t) = (t \pm \sqrt{q})^4$, then $A[\ell] \cong A(t^4, 0)$.*

Conversely, for any groupscheme G described above there exists an abelian variety B in the isogeny class of A such that $B[\ell] \cong G$.

Proof. Assume first that f_A has no multiple roots. Note that if $f_A(t) \equiv (t-\alpha)^3(t-\beta) \bmod \ell$, then $\alpha \equiv \beta \bmod \ell$. Thus by Corollaries 3.7 and 3.8 the cases $(1)-(3)$ and (5) follow. In the case (4) we have $A[\ell] \cong A(f_A, N)$, where N is a nilpotent 2×2-matrix, and N could be zero if and only if $R = \mathbb{Z}_\ell[t]/f_A(t)\mathbb{Z}_\ell[t]$ is not a DVR. Indeed, if R is regular, then $T_\ell(A)$ is free, and hence $N \neq 0$. If R is not regular, then the integral closure $\mathcal{O}$ of R is an example of an R-module such that $\mathcal{O}/\ell\mathcal{O} \cong A(f_A, 0)(\bar{k})$. By Dedekind lemma [ZP97, 5.55], R is regular if and only if $(f_A - h^2)/\ell$ is prime to h modulo ℓ. An easy computation shows that the two polynomials are coprime if and only if ℓ^2 does not divide $a_1^2 - 4a_2 + 8q$ for $\ell \neq 2$, and 4 does not divide $a_1 + a_2 + 1 - 2q$ for $\ell = 2$.

Assume now that f_A has multiple roots. It follows from the classification of Weil polynomials (see [MN02]), that only the cases $(6) - (8)$ are possible. The case (6) follows from the Proposition 3.9, and the case (8) is obvious since Frobenius acts by multiplication by $\mp\sqrt{q}$. By Corollary 3.7 conditions of $(7a)$, $(7b)$ and $(7c(i))$ are necessary. Let us prove the sufficiency. First

we construct Tate modules with the prescribed Frobenius action. The case $(7a)$ is obvious and in $(7b)$ $T_\ell(A) \cong T_1 \oplus T_2$, where T_i is a free module of rank 2 over $R_i = \mathbb{Z}_\ell[t]/P_i\mathbb{Z}_\ell[t]$. The module T_1 is uniquely determined, and T_2 can be constructed using Theorem 3.3.

In the case $(7c(i))$ we construct the Tate module as the sum $T_\ell(A) \cong T_1 \oplus T_2$, where T_1 is a module over $R_1 = \mathbb{Z}_\ell[t]/(t \pm \sqrt{q})\mathbb{Z}_\ell[t]$, and T_2 is a module over $R_2 = \mathbb{Z}_\ell[t]/P_1(t+\alpha)t\mathbb{Z}_\ell[t]$. By Theorem 3.3 for any 3×3 nilpotent matrix N such that $\mathrm{Np}(P_1(t+\alpha)t)$ lies on or above $\mathrm{Yp}(N)$ there exists an R_2-module T_2 such that F acts on $T_2/\ell T_2$ with the matrix $N \mp \sqrt{q}I_3$. Then $T = R_1 \oplus T_2$ is the desired Tate module.

Suppose now that we have a module T from the case $(7c(ii))$. Let $P(t) = tP_1(t \mp \sqrt{q})$. By Proposition 5.3 there exists a matrix factorization (X, Y) such that $\det X = f_A(t \mp \sqrt{q})$ and $YX = P(t)$. Moreover, $X \equiv \mathrm{diag}(t^2, t^2) \mod \ell$. Define T' by a presentation:

$$\mathbb{Z}_\ell[t]^2 \xrightarrow{Y} \mathbb{Z}_\ell[t]^2 \to T' \to 0, \tag{3}$$

Note that $\det Y = P(t)^2/f_A(t \mp \sqrt{q}) = P_1(t \mp \sqrt{q})$, and $Y \equiv \mathrm{diag}(t, t) \mod \ell$. Thus T' is a module over $R' = \mathbb{Z}_\ell[t]/P_1\mathbb{Z}_\ell[t]$. By Theorem 3.2 such a module exists iff $\mathrm{Np}(P_1(t \mp \sqrt{q}))$ lies on or above the Young polygon $(1, 1)$. It follows that if T exists then ℓ^2 divides $P_1(\mp\sqrt{q})$. On the other hand if ℓ^2 divides $P_1(\mp\sqrt{q})$, then we can construct a module T' over R' such that F acts on $T'/\ell T'$ with the matrix $\mp\sqrt{q}I_2$. By Proposition 5.3 there exists a matrix factorization (Y, X) such that $\det Y = P_1(t \mp \sqrt{q})$ and $XY = P(t)$. Then the matrix factorization (X, Y) corresponds to a desired module T. By Lemma 2.1 there exists an abelian variety B in the isogeny class of A such that $T \cong T_\ell(B)$. □

7. Kummer surfaces

Suppose $p \neq 2$. Let A be an abelian surface, and let $\tau : A \to A$ be an involution $a \mapsto -a$. Let $p_A : A \to A/\tau$ be the quotient map. The variety $X = A/\tau$ is singular, and $p_A(A[2])$ is the singular locus. Let $\sigma : S \to X$ be a blow up of $p_A(A[2])$. Then S is smooth. It is called a *Kummer surface*. In this section we compute zeta functions of Kummer surfaces in terms of the zeta functions of the covering abelian surfaces.

Let X be a variety over a finite field $\mathbb{F}_q$, and let N_d be the number of points of degree 1 on $X \otimes \mathbb{F}_{q^d}$. The zeta–function of X is a formal power series

$$Z_X(t) = \exp(\sum_{d=1}^{\infty} \frac{N_d t^d}{d}).$$

If X is smooth and projective, then $Z_X(t)$ is rational. For an abelian variety A we have the following formula:

$$Z_X(t) = \prod_{i=0}^{2g} P_i(t)^{(-1)^{i+1}}, \tag{4}$$

where $P_i(t) = \det(1 - tF | \bigwedge^i V_\ell(A))$. Note that if $f_A(t) = \prod(t - \omega_j)$, then

$$P_i(t) = \prod_{j_1 < \cdots < j_i} (1 - t\omega_{j_1} \ldots \omega_{j_i}).$$

In particular, $P_1(t) = t^{2g} f_A(\frac{1}{t})$, and $Z_A(t) = Z_B(t)$ if and only if A and B are isogenous.

First we prove a general formula for the zeta function of a Kummer surface S.

Theorem 7.1. *Let*

$$Z_A(t) = \prod_{i=0}^{4} P_i(A,t)^{(-1)^{i+1}}$$

be the zeta function of an abelian surface A. Then

$$Z_S(t) = (1-t)^{-1}P(t)^{-1}(1-q^2t)^{-1}, \tag{5}$$

where

$$P(t) = P_2(A,t)\prod_{a\in A[2]}(1-(qt)^{\deg a}). \tag{6}$$

In particular

$$|S(k)| = \frac{f_A(1)+f_A(-1)}{2} + q|A[2](k)| \tag{7}$$

Proof. Since S is a blow up of X, we have

$$Z_X(t) = Z_S(t)\prod_{a\in A[2]}(1-(qt)^{\deg a}).$$

Let us prove that

$$|X(\mathbb{F}_{q^r})| = \frac{f_r(1)+f_r(-1)}{2},$$

where $f_r = \det(t-F^r)$ is a Weil polynomial of $A_r = A\otimes\mathbb{F}_{q^r}$. Let $A(r) = A_r[2](\mathbb{F}_{q^r})$. It is well known that $f_A(n) = \deg(n-F)$ for $n\in\mathbb{Z}$, were deg means the degree of an isogeny [Mum70]. There are two types of possible fibers of the map p_A over a nonsingular $\mathbb{F}_{q^r}$-point of X.

(1) The fiber is a union of two points of degree 1. We have $\frac{f_r(1)-A(r)}{2}$ such fibers.
(2) The fiber is a point of degree 2. We have $\frac{f_r(-1)-A(r)}{2}$ such fibers.

This gives the desired equality.

Let $f_r(t) = t^4 + a_1(r)t^3 + a_2(r)t^2 + a_1(r)q^rt + q^{2r}$, then $a_2(r) = \mathrm{tr}(F^r|H^2(\bar{A},\mathbb{Q}_\ell))$, and

$$Z_X(t) = \exp(\sum_{r=1}^{\infty}\frac{(f_r(1)+f_r(-1))t^r}{2r}) =$$

$$\exp(\sum_{r=1}^{\infty}\frac{t^r}{r})\exp(\sum_{r=1}^{\infty}\frac{a_2(r)t^r}{r})\exp(\sum_{r=1}^{\infty}\frac{q^{2r}t^r}{r}) =$$

$$(1-t)^{-1}P_2(A,t)^{-1}(1-q^2t)^{-1}$$

The last equality follows from lemma C.4.1 of [Ha77]. □

Now we classify the zeta functions of $A[2]$ in terms of the Weil polynomial f_A. Let b_r be the number of points of degree r on $A[2]$. Then $P(t) = P_2(A,t)\prod_r(1-(qt)^r)^{b_r}$. We compute the numbers b_r using Theorem 6.1.

Suppose first that f_A has no multiple roots, and assume that $f_A(t)\equiv(t+1)^4 \bmod 2$. Note that the slopes of $\mathrm{Np}(f_A(t+1))$ may be greater than 1. This may create many unnecessary cases in the table below. However, we can use the polynomial $f(t) = f_A(t+\lambda)$ instead of $f_A(t+1)$, where $\lambda\equiv 1 \bmod \ell$, satisfy the property that slopes of $\mathrm{Np}(f(t))$ are less then or equal to 1. Equivalently, we take $\mathrm{Np}(f_A(t+1))$ and change all its slopes that are greater than 1 to 1. This operation simplifies the notation, and clearly, it does not change the final answer, since all the slopes of Young polygons are not greater than 1.

Table 1:

Slopes of $\mathrm{Np}(f(t))$	b_i
$(1/4)$	$b_1 = 2, b_2 = 1, b_4 = 3$
$(1/3, 1)$	$b_1 = 2, b_2 = 1, b_4 = 3$ $b_1 = 4, b_2 = 2, b_4 = 2$
$(1/2, 1/2)$	$b_1 = 2, b_2 = 1, b_4 = 3$ $b_1 = 4, b_2 = 2, b_4 = 2$ $b_1 = 4, b_2 = 6$
$(2/3, 1)$,$(1/2, 1, 1)$ or $(3/4)$	$b_1 = 2, b_2 = 1, b_4 = 3$ $b_1 = 4, b_2 = 2, b_4 = 2$ $b_1 = 4, b_2 = 6$ $b_1 = 8, b_2 = 4$
$(1, 1, 1, 1)$	$b_1 = 2, b_2 = 1, b_4 = 3$ $b_1 = 4, b_2 = 2, b_4 = 2$ $b_1 = 4, b_2 = 6$ $b_1 = 8, b_2 = 4$ $b_1 = 16$

If $f_A(t) \not\equiv (t+1)^4 \bmod 2$, then

Table 2:

$f_A(t) \bmod 2$	
$t^4 + t^3 + t^2 + t + 1$	$b_1 = 1, b_5 = 3$
$t^4 + t^3 + t + 1$ and 4 does not divide $f_A(1)$	$b_1 = 2, b_2 = 1, b_3 = 2, b_6 = 1$
$t^4 + t^3 + t + 1$ and 4 divides $f_A(1)$	$b_1 = 2, b_2 = 1, b_3 = 2, b_6 = 1$ $b_1 = 4, b_3 = 4$
$t^4 + t^2 + 1$ and 4 does not divide $a_1 + a_2 + 1 - 2q$	$b_1 = 1, b_3 = 1, b_6 = 2$
$t^4 + t^2 + 1$ and 4 divides $a_1 + a_2 + 1 - 2q$	$b_1 = 1, b_3 = 5$ $b_1 = 1, b_3 = 1, b_6 = 2$

If f_A has multiple roots, we have three cases of theorem 6.1. Let $f_A(t) = P_A(t)^2$ then there is the following table:

Table 3:

$P_A(t) \bmod 2$	
$t^2 + t + 1$	$b_1 = 1, b_3 = 5$
$t^2 + 1$ and 4 does not divide $P_A(1)$	$b_1 = 4, b_2 = 6$
$t^2 + 1$ and 4 divide $P_A(1)$	$b_1 = 4, b_2 = 6$ $b_1 = 8, b_2 = 4$ $b_1 = 16$

If $f_A(t) = (t \pm \sqrt{q})f(t)$, then the table looks as follows:

Table 4:

$f(t)$ mod 2	
$t^2 + t + 1$	$b_1 = 4, b_3 = 4$
$t^2 + 1$	$b_1 = 8, b_2 = 4$
and 4 does not divide $f(1)$	$b_1 = 4, b_2 = 2, b_3 = 2$
$t^2 + 1$	$b_1 = 16$
and 4 divide $f(1)$	$b_1 = 8, b_2 = 4$
	$b_1 = 4, b_2 = 6$
	$b_1 = 4, b_2 = 2, b_3 = 2$

Finally, if $f_A(t) = (t \pm \sqrt{q})^4$, we have $b_1 = 16$.

References

[BGK06] Banaszak G., Gajda W., Krason P. *On the image of l-adic Galois representations for abelian varieties of type I and II.* Doc. Math. Extra Volume Coats (2006), 35–75.

[De78] Demazure M., *Lectures on p-divisible groups*, Lecture notes in mathematics 302, Springer, 1972.

[Ha77] R. Hartshorne. *Algebraic geometry.* Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[HK71] K. Hoffman, R. Kunze. *Linear algebra.* (2nd Edition) Prentice Hall, 1971.

[KF67] *Algebraic number theory.* Proceedings of an instructional conference organized by the London Mathematical Society with the support of the Inter national Mathematical Union. Edited by J. W. S. Cassels and A. Frohlich. Academic Press, London; Thompson Book Co., Inc., Washington, D.C. 1967

[MN02] D. Maisner, E. Nart. *Abelian surfaces over finite fields as Jacobians.* With an appendix by Everett W. Howe. Experiment. Math. 11 (2002), no. 3, 321–337.

[Mil08] J. Milne, Abelian varieties. 2008. http://www.jmilne.org/math/CourseNotes/av.html

[Mum70] Mumford, David. *Abelian varieties.* Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Oxford University Press, London 1970

[Ry10] S. Rybakov. *The groups of points on abelian varieties over finite fields.* Cent. Eur. J. Math. 8(2), 2010, 282-288. arXiv:0903.0106v4

[Wa69] W. Waterhouse. *Abelian varieties over finite fields.* Ann. scient. Éc. Norm. Sup., 4 serie **2**, 1969, 521–560.

[WM69] W. Waterhouse, J. Milne. *Abelian varieties over finite fields.* Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969, 53–64.

[ZP97] M. Pohst, H. Zassenhaus. *Algorithmic algebraic number theory.* Revised reprint of the 1989 original. Encyclopedia of Mathematics and its Applications, 30. Cambridge University Press, Cambridge, 1997.

Poncelet laboratory (UMI 2615 of CNRS and Independent University of Moscow)

Institute for information transmission problems of the Russian Academy of Sciences
E-mail address: rybakov@mccme.ru, rybakov.sergey@gmail.com